ARITMÉTICA MODULAR

CONGRUENCIAS ENTERAS

Carl Friedrich Gauss (1777 – 1855)

Definición

Sean $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$.

a es congruente con b módulo m si y sólo si $m \mid a - b$.

$$a \equiv b \ (\text{mód } m)$$

La relación de congruencia es una relación de equivalencia:

1) reflexiva $a \equiv a \ (\text{mód } m)$
2) simétrica $a \equiv b \ (\text{mód } m)$ si y sólo si $b \equiv a \ (\text{mód } m)$
3) transitiva Si $a \equiv b \ (\text{mód } m)$, $b \equiv c \ (\text{mód } m)$ entonces $a \equiv c \ (\text{mód } m)$

Teorema

Sea $m \in \mathbb{N}$. Se verifican las siguientes propiedades:

1) $a \equiv b$ (mód m) si y sólo si $\boxed{a = m\,q + r,\ b = m\,q' + r}$ $0 \le r < m$.

Demostración

$\Leftarrow$) Si $a = m\,q + r$, $b = m\,q' + r \Rightarrow a - b = m\,(q - q') \Rightarrow m \mid a - b$
$\Leftrightarrow$ $a \equiv b$ (mód m).

$\Rightarrow$) Si $a = m\,q + r$, $b = m\,q' + r'$ con $0 \le r, r' < m$ y $a \equiv b$ (mód m)

entonces $m \mid a - b = m\,(q - q') + (r - r') \Rightarrow m \mid r - r' \Rightarrow$

$\exists\, k \in \mathbb{Z}$ tal que $r - r' = m\,k$, luego,

$$\begin{cases} a = m\,q + r = m\,q + m\,k + r' = m\,(q + k) + r' \Rightarrow r \le r' \\ b = m\,q' + r' = m\,q' - mk + r = m(q' - k) + r \Rightarrow r' \le r \end{cases} \Rightarrow r = r'$$

2) $\forall\, a \in \mathbb{Z}, \exists\ r\ \in \{0, 1, 2, \ldots, m-1\}$ tal que $\boxed{a \equiv r\ (\text{mód } m)}$

Demostración

$\forall\, a \in \mathbb{Z}\,, \exists\, q, r \in \mathbb{Z}$ tales que $a = m\,q + r$ con $0 \le r < m \Rightarrow$

$m \mid a - r \Leftrightarrow a \equiv r\ (\text{mód } m)$.

Definiciones

- Clase de congruencias módulo m es el conjunto

$$[r]_m = \{\, a \in \mathbb{Z} \,/\, a \equiv r\ (\text{mód } m)\} = \{\, a \in \mathbb{Z} \,/\, \exists\, q \in \mathbb{Z}\,,\ a = m\,q + r\}$$

- Conjunto de mínimos restos no negativos módulo m

$$\mathbb{Z}_m = \{\, [0]_m\,,\, [1]_m\,,\, \ldots\,,\, [m-1]_m\,\}$$

Ejemplo

- Clase de congruencias módulo 6 es el conjunto

$$[r]_6 = \{ a \in \mathbb{Z} / a \equiv r \,(\text{mód } 6)\} = \{ a \in \mathbb{Z} / \exists\, q \in \mathbb{Z}\,,\, a = 6q + r\}$$

- Conjunto de mínimos restos no negativos módulo 6

$$\mathbb{Z}_6 = \{ [0]_6\,, [1]_6\,, [2]_6, [3]_6\,, [4]_6, [5]_6\}$$

$$[0]_6 = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}$$

$$[1]_6 = \{\ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\}$$

$$[2]_6 = \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\}$$

$$[3]_6 = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\}$$

$$[4]_6 = \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\}$$

$$[5]_6 = \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\}$$

Proposición

La relación de congruencia es compatible con la suma y el producto en $\mathbb{Z}$

Si $a \equiv b \ (\text{mód } m)$ y $c \equiv d \ (\text{mód } m)$ entonces $\begin{cases} a + c \equiv (b + d) (\text{mód } m) \\ a\, c \equiv (b\, d) (\text{mód } m) \end{cases}$

Demostración

Si $a \equiv b \ (\text{mód } m)$ entonces $m \mid a - b$

$c \equiv d \ (\text{mód } m)$ entonces $m \mid c - d$

Se tiene que

- $m \mid (a + c) - (b + d) \Rightarrow a + c \equiv (b + d) (\text{mód } m)$
- $m \mid a\, c - b\, c$ y $m \mid b\, c - b\, d \Rightarrow m \mid a\, c - b\, d \Rightarrow a\, c \equiv (b\, d) (\text{mód } m)$

Definición

Se definen las siguientes operaciones en $\mathbb{Z}_m$

suma: $[a]_m + [b]_m = [a+b]_m$

producto: $[a]_m \, [b]_m = [a\,b]_m$

que verifican las siguientes propiedades

	suma	producto
asociativa	$[a] + [b + c] = [a + b] + [c]$	$[a]\,[b\,c] = [a\,b]\,[c]$
conmutativa	$[a + b] = [b + a]$	$[a\,b] = [b\,a]$
existencia de elemento neutro	$[a] + [0] = [a]$	$[a]\,[1] = [a]$
existencia de elementos opuestos	$\forall\, [a] \in \mathbb{Z}_m \quad \exists - [a] = [-a] \in \mathbb{Z}_m$ tal que $[a] + [-a] = [0]$	
distributiva	$[a]\,[b + c] = [a]\,[b] + [a]\,[c]$	

Suma en $\mathbb{Z}_5$

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

Producto en $\mathbb{Z}_5$

*	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Suma en $\mathbb{Z}_6$

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Producto en $\mathbb{Z}_6$

*	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

En $\mathbb{Z}_m$ no siempre se cumple la propiedad cancelativa:

$$[6]_8\ [4]_8 = [0]_8 = [4]_8\ [4]_8$$

$$[6]_8 \neq [4]_8$$

Proposición

Si $a\,c \equiv b\,c\ (\text{mód}\ m)$, $c \neq 0$, entonces $\boxed{a \equiv b \mod \left(\frac{m}{\text{mcd}\,(m,c)}\right)}$

Demostración

$a\,c \equiv b\,c\ (\text{mód}\ m) \Leftrightarrow m \mid a\,c - b\,c = (a-b)\,c.$ Si $d = \text{mcd}\,(m, c)$

entonces $\frac{m}{d}, \frac{c}{d} \in \mathbb{Z}$, $\frac{m}{d} \mid (a-b)\frac{c}{d}$ y $mcd\left(\frac{m}{d}, \frac{c}{d}\right) = 1 \Rightarrow$

$\frac{m}{d} \mid (a-b) \Leftrightarrow a \equiv b \mod \left(\frac{m}{d}\right)$

Ejemplo

Se tiene que $432 \equiv 32$ (mód 80)

$c = \text{mcd}\,(432, 32) = 16$

$d = \text{mcd}\,(80, 16) = 16$

$$\frac{432}{16} \equiv \frac{32}{16} \bmod \left(\frac{80}{mcd(80,16)}\right)$$

$$27 \equiv 2 \pmod 5$$

Consecuencia

$\mathbb{Z}_m$ tiene la propiedad cancelativa si m es primo.

Definición

$[a]_m \in \mathbb{Z}_m$ es inversible en $\mathbb{Z}_m$ si $\exists\ [b]_m \in \mathbb{Z}_m$ tal que $[a]_m\,[b]_m = [1]_m$

Proposición

$[a]_m$ tiene inverso en $\mathbb{Z}_m$ si y sólo si mcd $(a, m) = 1$

Demostración

$[a]_m$ tiene inverso en $\mathbb{Z}_m \Leftrightarrow$

$\exists\ [b]_m \in \mathbb{Z}_m$ tal que $[a]_m[b]_m = [1]_m$ o tal que $a\,b \equiv 1$ (mód m) $\Leftrightarrow$

$\exists\ [b]_m \in \mathbb{Z}_m$ y $\exists\ q \in \mathbb{Z}$ tal que $a\,b - 1 = m\,q$ o $a\,b - m\,q = 1 \Leftrightarrow$

mcd $(a, m) = 1$

Ejemplo

$[x]_{80}$ es el inverso de $[7]_{80}$ en $\mathbb{Z}_{80}$ $\Leftrightarrow$ $[7]_{80}\,[x]_{80} = [1]_{80}$

$\Leftrightarrow \exists\ y \in \mathbb{Z}$ tal que $7x - 80y = 1$.

Aplicando el algoritmo de Euclides

$80 = 7.11 + 3$

$7 = 3.2 + 1$

$3 = 1.3$

$\text{mcd}\,(80, 7) = 1 = 7 - 3.2 = 7 - (80 - 7.11).2 = -80.2 + 23.7$

La solución general es $\begin{cases} x = 23 + 80t \\ y = 2 + 7t \end{cases} \quad \forall t \in \mathbb{Z}$

Por tanto, $[x]_{80} = [23]_{80}$ es el inverso de $[7]_{80}$ en $\mathbb{Z}_{80}$

CRITERIOS DE DIVISIBILIDAD

Sea $x = (x_n\, x_{n-1} \ldots x_1\, x_0)_{10}$ la representación decimal del número entero

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \ldots + 10\, x_1 + x_0 = \sum_{i=0}^{n} 10^i x_i$$

1) Divisibilidad por 2 y por 5:

$x = 10\,(10^{n-1} x_n + 10^{n-2} x_{n-1} + \ldots + x_1) + x_0 \Rightarrow x \equiv x_0 \text{ (mód 10)} \Rightarrow$

- $x \equiv x_0$ (mód 2). Luego, $2 \mid x$ si y sólo si $2 \mid x_0$
- $x \equiv x_0$ (mód 5). Luego, $5 \mid x$ si y sólo si $5 \mid x_0$

2) Divisibilidad por 3 y por 9:

$$x - \sum_{i=0}^{n} x_i = \sum_{i=0}^{n} (10^i - 1)\, x_i = 9\, x_1 + 99\, x_2 + \ldots + 9\ldots9\, x_n \equiv 0 \text{ (mód 9)} \Rightarrow$$

- $x \equiv \sum_{i=0}^{n} x_i$ (mód 9). Luego, $9 \mid x$ si y sólo si $9 \mid \sum_{i=0}^{n} x_i$
- $x \equiv \sum_{i=0}^{n} x_i$ (mód 3). Luego, $3 \mid x$ si y sólo si $3 \mid \sum_{i=0}^{n} x_i$

3) Divisibilidad por 4:

$$x = 100\,(10^{n-2}\, x_n + 10^{n-3}\, x_{n-1} + \ldots + x_2) + (10\, x_1 + x_0) \Rightarrow$$

$$x \equiv (10\, x_1 + x_0) \text{ (mód 100)} \Rightarrow x \equiv (10\, x_1 + x_0) \text{ (mód 4).}$$

Luego, $4 \mid x$ si y sólo si $4 \mid (10\, x_1 + x_0)$

4) Divisibilidad por 11:

$$\begin{cases} 10^j \equiv 1 \pmod{11}, \text{si } j \text{ es par} \\ 10^j \equiv -1 \pmod{11}, \text{si } j \text{ es impar} \end{cases} \Rightarrow$$

$$x = \sum_{j=0}^{n} 10^j x_j \equiv \sum_{j=0}^{n} (-1)^j x_j \pmod{11}$$

Luego, $11 \mid x$ si y sólo si $11 \mid \sum_{j=0}^{n} (-1)^j x_j$.

5) Divisibilidad por 7:

$$x \equiv [(x_0 + 3\,x_1 + 2\,x_2) - (x_3 + 3\,x_4 + 2\,x_5) + (x_6 + 3\,x_7 + 2\,x_8) - \ldots] \pmod{7}$$

Demostración

$$x - (x_0 + 3\,x_1 + 2\,x_2\,) + (x_3 + 3\,x_4 + 2\,x_5\,) - (x_6 + 3\,x_7 + 2\,x_8\,) + \ldots =$$

$$= (x_0 + 10\,x_1 + 100\,x_2 + \ldots + 10^{n-1}\,x_{n-1} + 10^{n}\,x_n) - (x_0 + 3\,x_1 + 2\,x_2\,) +$$

$$(x_3 + 3\,x_4 + 2\,x_5\,) - \ldots = 7\,x_1 + 98\,x_2 + 1001\,x_3 + 10003\,x_4 + 100002\,x_5 + \ldots$$

que es múltiplo de 7

Luego, $7 \mid x$ si y sólo si $7 \mid (\,x_0 + 3\,x_1 + 2\,x_2\,) - (x_3 + 3\,x_4 + 2\,x_5\,) + \ldots$

REGLA DEL NUEVE

Sea $x = (x_n\, x_{n-1} \ldots x_1\, x_0)_{10}$ la representación decimal del número entero

$$x = 10^n x_n + 10^{n-1} x_{n-1} + \ldots + 10\, x_1 + x_0 = \sum_{i=0}^{n} 10^i x_i$$

Sean $a, b, c, q, r \in \mathbb{Z}$,

a) Si $c = a\, b$ entonces $\sum_{i=0}^{n} a_i . \sum_{i=0}^{n} b_i \equiv \sum_{i=0}^{n} c_i \pmod 9$

b) Si $a = b\, q + r$ entonces $\sum_{i=0}^{n} b_i \sum_{i=0}^{n} q_i + \sum_{i=0}^{n} r_i \equiv \sum_{i=0}^{n} a_i \pmod 9$

UNIDADES EN $\mathbb{Z}_m$

Leonhard Euler (1707 – 1783)

Definición

Conjunto de unidades de $\mathbb{Z}_m$ es el conjunto

$$U_m = \{ [a]_m \in \mathbb{Z}_m \,/\, [a]_m \text{ es inversible} \}$$

$$U_m = \{ [a]_m \in \mathbb{Z}_m \,/\, \text{mcd}\,(a, m) = 1 \}$$

Propiedades

1) Si $[a]_m , [b]_m \in U_m$, entonces $[a\,b]_m \in U_m$

$$[a\,b]_m^{-1} = [a]_m^{-1}\,[b]_m^{-1}$$

2) Si $[a]_m \in U_m$, entonces $[a]_m\, U_m = U_m$

Demostración

$\subseteq$) Si $[z]_m \in [a]_m \, U_m \Rightarrow \exists \, [b]_m \in U_m$ tal que $[z]_m = [a]_m[b]_m = [a\ b]_m \in U_m$

$\supseteq$) Si $[z]_m \in U_m \Rightarrow [z]_m = ([a]_m \, [a]_m^{-1}) \, [z]_m = [a]_m \, ([a]_m^{-1}[z]_m) \in [a]_m \, U_m$

Ejemplo

$(U_8, *)$	$\mathbf{[1]_8}$	$\mathbf{[3]_8}$	$\mathbf{[5]_8}$	$\mathbf{[7]_8}$
$\mathbf{[1]_8}$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$\mathbf{[3]_8}$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$\mathbf{[5]_8}$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$\mathbf{[7]_8}$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

Proposición

Si p es primo entonces los únicos elementos que coinciden con su inverso en $\mathbb{Z}_p$ son $[1]_p$ y $[-1]_p$.

Demostración

Si $[a]_p^{-1} = [a]_p$, entonces $[a^2]_p = [1]_p$, es decir que $a^2 \equiv 1$ (mód p).

$p \mid a^2 - 1 = (a-1)(a+1)$, entonces $\begin{cases} p \mid a-1 \Rightarrow a \equiv 1 (\text{mod } p) \\ p \mid a+1 \Rightarrow a \equiv -1 (\text{mod } p) \end{cases}$

Teorema de Wilson (1770)

Si p es primo entonces $(p-1)! \equiv (p-1)$ (mód p)

Ejemplo

Halla el resto de dividir 11! entre 13 y entre 17.

- $p = 13$, entonces como $(p-1)! \equiv -1 (\text{mód } p) \Rightarrow 12! \equiv 12 \text{ (mód 13)}$

  $\Leftrightarrow 11! \equiv 1 \text{ (mód 13)}$

- $p = 17$, entonces como $(p-1)! \equiv -1 (\text{mód } p) \Rightarrow 16! \equiv 16 \text{ (mód 17)}$

  $\Leftrightarrow 15! \equiv 1 \text{ (mód 17)} \Leftrightarrow 15.14.13.12.11! \equiv 1 \text{ (mód 17)}$

$$11! \equiv 15^{-1}.14^{-1}.13^{-1}.12^{-1} \text{ (mód 17)}$$

$$11! \equiv 8.11.4.10 \text{ (mód 17)} = 1 \text{ (mód 17)}$$

Función de Euler

Sea $K_n = \{k \in \mathbb{N} \ / \ 1 \leq k \leq n, \ \text{mcd}\,(k, n) = 1\}$.

Se define la función de Euler $\Phi: \mathbb{N} \to \mathbb{N}$ tal que

- $\Phi(n) = \text{card}\, K_n = \text{card}\, \{ k \in \mathbb{N} \ / \ 1 \leq k \leq n, \ \text{mcd}\,(k, n) = 1 \}$
- $\Phi(n) = \text{card}\, U_n = \text{card}\, \{ [a]_n \in \mathbb{Z}_n \ / \ \text{mcd}\,(a, n) = 1 \}$

Propiedades

1) Si p es primo, entonces $\Phi(p) = p - 1$

Demostración

$\Phi(p) = \text{card}\, U_p = \text{card}\, (\mathbb{Z}_p - [0]_p) = p - 1$

2) Si p es primo, entonces $\Phi(p^r) = p^r - p^{r-1}, \ \forall \ r \in \mathbb{N}$

Demostración

$\Phi(p^r) = \text{card } U_{p^r} = \text{card}\left\{ [a]_{p^r} \in \mathbb{Z}_{p^r} \text{ tal que } \text{mcd}(a, p^r) = 1 \right\} =$

$= \text{card } \mathbb{Z}_{p^r} - \text{card}\left\{ [a]_{p^r} \in \mathbb{Z}_{p^r} \text{ tal que } \text{mcd}(a, p^r) \neq 1 \right\} = p^r - p^{r-1}$

ya que los únicos números no primos con p^r son

$\{ p, 2p, 3p, ..., pp, ..., p^2 p, ..., p^{r-1} p \}$

3) Si $\text{mcd}(a, b) = 1$ entonces $\Phi(a\,b) = \Phi(a)\,\Phi(b)$

4) Si $n = p_1^{r_1} \ldots p_k^{r_k}$ con p_i números primos distintos, entonces

$$\Phi(n) = \Phi(p_1^{r_1} \ldots p_k^{r_k}) = \Phi(p_1^{r_1}) \ldots \Phi(p_k^{r_k}) = \left(p_1^{r_1} - p_1^{r_1-1}\right) \ldots \left(p_k^{r_k} - p_k^{r_k-1}\right) =$$

$$= p_1^{r_1}\left(1-\frac{1}{p_1}\right) \ldots p_k^{r_k}\left(1-\frac{1}{p_k}\right) = n\left(1-\frac{1}{p_1}\right) \ldots \left(1-\frac{1}{p_k}\right)$$

Ejemplo

$$\Phi(12) = \Phi(2^2\, 3) = \Phi(2^2)\,\Phi(3) = (2^2-2).2 = 4$$

$$\Phi(12) = \Phi(2^2\, 3) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 4$$

Teorema de Euler

- Si $[a]_m \in \mathrm{U}_m$, entonces $[a]_m^{\Phi(m)} = [1]_m$
- Si mcd $(a, m) = 1$, entonces $a^{\Phi(m)} \equiv 1 \ (\text{mód } m)$.

Demostración

Si $\mathrm{U}_m = \{ [x_1]_m, [x_2]_m, ..., [x_k]_m \}$ entonces $\Phi(m) = \text{card } \mathrm{U}_m = k$.

Si $[a]_m \in \mathrm{U}_m$ entonces $[a]_m \mathrm{U}_m = \mathrm{U}_m$ y por tanto,

$$\{ [a\,x_1], [a\,x_2], ..., [a\,x_k] \} = \{ [x_1], [x_2], ..., [x_k] \}$$

Luego, $[a\,x_1]\,[a\,x_2] \ldots [a\,x_k] = [x_1]\,[x_2] \ldots [x_k] \Leftrightarrow$

$[a^k]\,[x_1]\,[x_2] \ldots [x_k] = [x_1]\,[x_2] \ldots [x_k] \Rightarrow [a^k] = [1] \Leftrightarrow a^k \equiv 1 \ (\text{mód } m)$.

Ejemplo

Halla el resto de la división entera de $13^{22}\ 27^{41}$ entre 8.

$\Phi(8) = \Phi(2^3) = 2^3 - 2^2 = 4$

- $13^{\Phi(8)} = 13^4 \equiv 1 \text{ (mód 8)}$

  $13^{22} = (13^4)^5\ 13^2 \equiv 13^2 \text{ (mód 8)} \equiv 5^2 \text{ (mód 8)} \equiv 1 \text{ (mód 8)}$

- $27^{\Phi(8)} = 27^4 \equiv 1 \text{ (mód 8)}$

  $27^{41} = (27^4)^{10}\ 27 \equiv 27 \text{ (mód 8)} \equiv 3 \text{ (mód 8)}$

- $13^{22}\ 27^{41} \equiv 3 \text{ (mód 8)}$